ABSTRAK

Administrator memiliki tanggung jawab yang besar dalam upaya pengamanan jaringan , sistem , serta data , dan membuat berbagai upaya untuk melakukan tindakan pengamanan. Umumnya *administrator* menggunakan *firewall* sebagai dinding pertahanan. Namun *firewall* tidak dirancang untuk memberikan notifikasi detail dari serangan. Kemudian berkembanglah teknologi *IPS (Intrusion Prevention System)* yang berfungsi untuk mendeteksi adanya serangan dari penyusup kemudian memberikan peringatan berupa notifikasi serta melakukan respon aktif dengan mem*block* alamat *IP* penyerang. Sistem ini akan mempermudah *administrator* mengetahui sejak dini apabila telah terjadi serangan pada sistem komputer di jaringan tersebut.

Ossec Hids, adalah salah satu *IPS* yang digunakan untuk mendeteksi sistem dari aktifitas-aktifitas yang dianggap mengancam dan kemudian membuat *log* dan mampu memberikan peringatan berupa notifikasi *via email* ke *system administrator* dan dapat memberikan respon dengan mem*block* alamat *IP* penyerang.

Pada proyek akhir ini akan dibangun sistem pertahanan menggunakan aplikasi *Ossec Hids* yang akan diuji dengan beberapa metode penyerangan seperti *port scanning* , *brute-force attack* , *rootkit* , dan *DDOS attack*. Diharapkan dengan diimplementasikannya *Ossec Hids* dapat mendeteksi sejak awal jika terjadi indikasi serangan dan memberikan respon aktif dengan mem*block* alamat *IP* penyerang. Sehingga mempermudah *administrator* memantau keamanan sistemnya.

Kata kunci : *Ossec Hids* , *IPS* , *port scanning* , *brute-force attack* , *rootkit* , *DDOS*

ABSTRACT

Administrator has a big responsibility to secure networks, a system, and data. It also does the security precautions. Generally, administrator uses a firewall as the wall of defense. However, firewall is not designed to give detailed notifications from the attack. Because of it, IPS (Intrusion Prevention System) is developed. It is functioned to detect the presence of an intruder attack and then give a warning notification and makes an active response by blocking the ip address of the attacker. This system makes the administrator easier to know it, if there is an attack in computer system.

Ossec Hid is one of the IPS used to detect the system from its activities that many threaten, make a log and be able to give a warning notification via email to the administrator and be able to give a respond by blocking the IP address of attacker.

The result of My final project is a security system using Ossec Hids, will be test using port scanning , brute-force attack , rootkit , and DDoS attack. By the implementation of Ossec Hids, it is expected to detect indications of the attack earlier to give an active response by blocking ip address of the attacker. So, it will make the administrator easier to monitor the security system.

Keywords : Ossec Hids , IPS , Port Scanning , Brute-force attack , Rootkit , DDoS.